[10191/1739]

A KEY VERIFICATION METHOD

FIELD OF THE INVENTION

The present invention relates to a key verification method and a security system.

BACKGROUND INFORMATION

Passive security systems are available for vehicles which use remote keys having transponders that communicate with a transceiver of a vehicle, when the transponder is within range of the transceiver. Provided communication between a key and the transceiver follows a predetermined communications protocol, and unique authentication data is exchanged and validated, the key is considered a valid key and the system allows entry to and/or use of the vehicle. When the valid key subsequently moves out of range of the transceiver, the security system secures the vehicle by locking and immobilizing the vehicle.

When a valid key for a vehicle becomes lost, the key needs to be deactivated so it can no longer be used to gain access to the vehicle. Accordingly, it is desired to provide a simple technique for deactivating lost keys and reactivating found valid keys, particularly when the keys are buttonless.

SUMMARY OF THE INVENTION

In an exemplary embodiment of the present invention, there is

provided an exemplary key verification method for a security system including at least one valid key and an electronic control apparatus, arrangement or unit with a transceiver for communicating with the at least one valid key. The control apparatus, arrangement or unit generates an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, this method including accessing the unique identification data for the at least one valid key in a mode of the system.

The exemplary method includes storing enable data corresponding to the unique identification data for the at least one valid key, a user executing a predetermined procedure to enter a key validation mode of the system, and in the validation mode retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, keys without the enable data being deactivated for the system.

The exemplary embodiment of the present invention also provides a security system including at least one valid key and electronic control apparatus, arrangement or unit with a transceiver for communicating with the at least one valid key, the control apparatus, arrangement or unit generating an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the system having a mode for accessing the unique identification data for the at least one valid key.

In an exemplary embodiment, the control apparatus, arrangement or unit stores enable data corresponding to the unique identification data for the at least one valid key when activated for the system, and the control apparatus, arrangement or unit enters a key validation mode when a user executes a predetermined procedure, and in the validation mode the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the transceiver.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a block diagram of an exemplary embodiment of a security system.

DETAILED DESCRIPTION

A security system, as shown in Figure 1, includes an electronic control unit (ECU) 2, which is mounted in a vehicle and includes processing circuitry to communicate with other electrical and electronic components of the vehicle and the security system. In particular, ECU 2 includes an rf transceiver 14 for generating an rf signal which excites the transponder of a remote key 4 of the security system when key 4 is within the vicinity of a vehicle. Key 4 may have a card or fob. Once excited, key 4 uses rf transmission techniques to communicate with the transceiver, in accordance with a secure communications protocol, in order to pass authentication data from key 4 to ECU 2. Once received, ECU 2 compares the authentication data with security data that it holds in its memory, these being security codes and enable flags stored in an EEPROM 12. When ECU 2 finds a match between the received authentication data and its own security data, ECU 2 issues

signals to other components of the vehicle to enable access to and/or operation of the vehicle by the holder of key 4. When key 4 is removed from the immediate vicinity of the vehicle, this is detected by transceiver 14, which causes ECU 2 to generate signals to secure the vehicle, for example by locking and immobilizing the vehicle.

Normally, a number of valid keys can be used with the security system to gain access to the vehicle. Keys 4 each include a unique serial or identification number and this is communicated to ECU 2 as part of the authentication data. ECU 2 stores the serial numbers for each valid key in its EEPROM 12, and an enable flag is stored against each serial number. As an alternative to the enable flag, the system can store a control byte which may be an encoded version of the identification number. During the authentication procedure when ECU 2 verifies the authentication data, ECU 2 checks to determine whether the received serial number of the communicating key 4 is stored in EEPROM 12 and whether its enable flag is set or reset. If the serial number is found and the enable flag is set, then the communicating key constitutes a valid key which can be used to gain access to the vehicle. If however the serial number is found and the enable flag is not set, then the communicating key is no longer a valid key which can be used. The ECU 2 is capable of deactivating the key and carrying out an activation procedure which resets and sets the enable flag for key 4. This enables a vehicle owner whose keys have been lost or stolen to proceed in a simple manner as described above.

If a valid key has been lost or stolen, the holder of at least

one remaining valid key can set ECU 2 to a key validation mode in order to validate all the remaining keys. The holder of the remaining keys simply enters the vehicle, brings all the remaining keys within range of transceiver 14, and executes a predetermined procedure to put ECU 2 into the key validation mode. When ECU 2 is in the key validation mode, ECU 2 turns on all the keys 4 within its range in order to receive their serial numbers and sets the enable flags in EEPROM 12 for the received serial numbers, while the enable flags for all the other key serial numbers stored in EEPROM 12 are reset. The keys within range of transceiver 14 will then represent valid keys and the lost or stolen key will no longer be a valid key, since its enable flag is reset. The ECU 2 displays the completion of the key validation procedure by generating a completion signal for a message unit 6. The message unit simply shows either visually or acoustically that the key validation procedure has been completed. Message unit 6 may be an LED in the vehicle or a horn or a siren of the vehicle. Message unit 6 may also be a display unit in the vehicle, which receives the data and is capable of showing which keys are valid for the vehicle. The display unit could also display other messages, such as, for example "Key validation completed," and may include controls allowing a user of the vehicle to recall a display showing the valid keys, for example, key A, B, and C.

If the lost or stolen key 4 is recovered, the key can be revalidated or reactivated by bringing all the keys into the vehicle again and placing ECU 2 in the key validation mode in order to execute the above-explained key validation procedure. The enable flag for the found key 4 will then be set in EEPROM

To avoid the requirement for any additional hardware components to be added to the vehicle, the predetermined procedure used to place ECU 2 in the key validation mode needs to be executed (or performed) using existing (or standard) vehicle components. The predetermined procedure should advantageously involve using components and operations which are normally involved in a start or entry procedure for the vehicle. Vehicles may have a start procedure which involves pressing a pedal 8, which may be the brake or clutch pedal, and then simultaneously turning on an ignition start switch 10 of the vehicle. The ECU 2 is connected to the electric network or wiring harness of the vehicle so as to receive signals generated when pedal 8 is depressed and ignition start switch 10 is turned on. The predetermined procedure to enter the key validation mode can then involve the holder of the keys simply depressing pedal 8 and turning on ignition start switch 10 alternately a number of times, say three times, instead of doing this simultaneously. The ECU 2 on detecting depression of pedal 8 and turning on of ignition start switch 10 alternately can then generate a message for message unit 6 to confirm entry into the key validation mode when the predetermined procedure has been executed. The ECU 2 can also issue cues on message unit 6 to follow the time sequence for depression of pedal 8 and turning on ignition start switch 10, to assist the holder of the keys in correctly executing the procedure to enter the key validation mode. Alternatively, the steps and vehicle components used for entry into the vehicle can be used; for example, in some passive security systems the key is excited on lifting a door handle 16. The

predetermined procedure required to enter the key validation mode may require a holder of the keys to lift door handle 16 a number of times within a certain period of time, for example four times in two seconds.

The ECU 2 can be provided by or divided into a number of ECUs, and similarly the vehicle can include a number of transceivers and antennas to communicate with remote keys 4. Keys 4 may be passive entry keys which require energy from the vehicle in order to communicate with ECU 2 or the keys may have their own battery power supply. Also, while the exemplary methods and embodiments of the present inventions are believed to be particularly advantageous for keys which have no activating buttons, keys 4 can include activating buttons and the security system may be a combination of active and passive security systems. For example, the security system may be designed such that key 4 is able to communicate over a distance, of for example 30 m, with the vehicle when activated, and is also able to be energized or excited when closer to the vehicle by, for example, lifting the door handle, or some other activation device, when in the vicinity of the vehicle.

ABSTRACT OF THE DISCLOSURE

A key verification method for a security system, which includes one valid key and an electronic verification control with a transceiver for communicating with the valid key, includes using the electronic verification control for generating an authority for access to a secured object when authentication data is received from the valid key and storing unique identification data for the valid key, accessing the unique identification data for the valid key in one mode of the system by storing enable data corresponding to the unique identification data for the valid key, executing or performing a predetermined procedure to enter a key validation mode of the system, and, in the validation mode, retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, and deactivating keys without the enable data for the system. Also described is a security system including one valid key and an electronic verification control with a transceiver for communicating with the valid key, in which the electronic verification control includes a mode for accessing the unique identification data for the valid key, and generating an authority for access to a secured object when authentication data is received from the valid key and storing unique identification data for the valid key enabling data corresponding to the unique identification data for the valid key when activated for the system, entering a key validation mode when a user executes a predetermined procedure, and, in the validation mode, retaining the enable data for valid keys within range of the transceiver and deleting it for valid keys out of range of the transceiver.

353922

A KEY VERIFICATION METHOD

The present invention relates to a key verification method and a security system.

Passive security systems are available for vehicles which use remote keys having transponders that communicate with a transceiver of a vehicle, when the transponder is within range of the transceiver. Provided communication between a key and the transceiver follows a predetermined communications protocol, and unique authentication data is exchanged and validated, the key is considered a valid key and the system allows entry to and/or use of the vehicle. When the valid key subsequently moves out of range of the transceiver, the security system secures the vehicle by locking and immobilizing the vehicle.

When a valid key for a vehicle becomes lost, the key needs to be deactivated so it can no longer be used to gain access to the vehicle. Accordingly, it is desired to provide a simple technique for deactivating lost keys and reactivating found valid keys, particularly when the keys are buttonless.

In accordance with the present invention, there is provided a key verification method for a security system including at least one valid key and electronic control means with a transceiver for communicating with the at least one valid key, the control means generating an authority for access to a

secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, this method including accessing the unique identification data for the at least one valid key in a mode of the system;

characterized by storing enable data corresponding to the unique identification data for the at least one valid key, a user executing a predetermined procedure to enter a key validation mode of the system, and in the validation mode retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, keys without the enable data being deactivated for the system.

The present invention also provides a security system including at least one valid key and electronic control means with a transceiver for communicating with the at least one valid key, the control means generating an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the method having a mode for accessing the unique identification data for the at least one valid key;

characterized in that the control means stores enable data corresponding to the unique identification data for the at least one valid key when activated for the system, and the control means enters a key validation mode when a user executes a predetermined procedure, and in the validation mode the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the

transceiver.

A preferred embodiment of the present invention is hereinafter described, by way of example, with reference to the accompanying drawing, wherein:

Figure 1 is a block diagram of a preferred embodiment of a security system.

A security system, as shown in Figure 1, includes an electronic control unit (ECU) 2, which is mounted in a vehicle and includes processing circuitry to communicate with other electrical and electronic components of the vehicle and the security system. In particular, ECU 2 includes an rf transceiver 14 for generating an rf signal which excites the transponder of a remote key 4 of the security system when key 4 is within the vicinity of a vehicle. Key 4 may have a card or fob. Once excited, key 4 uses rf transmission techniques to communicate with the transceiver, in accordance with a secure communications protocol, in order to pass authentication data from key 4 to ECU 2. Once received, ECU 2 compares the authentication data with security data that it holds in its memory, these being security codes and enable flags stored in an EEPROM 12. When ECU 2 finds a match between the received authentication data and its own security data, ECU 2 issues signals to other components of the vehicle to enable access to and/or operation of the vehicle by the holder of key 4. When key 4 is removed from the immediate vicinity of the vehicle, this is detected by transceiver 14, which causes ECU 2 to generate signals to secure the vehicle, for example by locking and immobilizing the vehicle.

Normally, a number of valid keys can be used with the security system to gain access to the vehicle. Keys 4 each include a unique serial or identification number and this is communicated to ECU 2 as part of the authentication data. ECU 2 stores the serial numbers for each valid key in its EEPROM 12, and an enable flag is stored against each serial number. As an alternative to the enable flag, the system can store a control byte which may be an encoded version of the identification number. During the authentication procedure when ECU 2 verifies the authentication data, ECU 2 checks to determine whether the received serial number of the communicating key 4 is stored in EEPROM 12 and whether its enable flag is set or reset. If the serial number is found and the enable flag is set, then the communicating key constitutes a valid key which can be used to gain access to the vehicle. If however the serial number is found and the enable flag is not set, then the communicating key is no longer a valid key which can be used. ECU 2 is capable of deactivating the key and carrying out an activation procedure which resets and sets the enable flag for key 4. This enables a vehicle owner whose keys have been lost or stolen to proceed in a simple manner as described above.

If a valid key has been lost or stolen, the holder of at least one remaining valid key can set ECU 2 to a key validation mode in order to validate all the remaining keys. The holder of the remaining keys simply enters the vehicle, brings all the remaining keys within range of transceiver 14, and executes a predetermined procedure to put ECU 2 into the key validation mode. When ECU 2 is in the key validation mode, ECU 2 turns on all the keys 4 within its range in order to receive their serial numbers and sets the enable flags in EEPROM 12 for the

received serial numbers, while the enable flags for all the other key serial numbers stored in EEPROM 12 are reset. The keys within range of transceiver 14 will then represent valid keys and the lost or stolen key will no longer be a valid key, since its enable flag is reset. ECU 2 displays the completion of the key validation procedure by generating a completion signal for a message unit 6. The message unit simply shows either visually or acoustically that the key validation procedure has been completed. Message unit 6 may be an LED in the vehicle or a horn or a siren of the vehicle. Message unit 6 may also be a display unit in the vehicle, which receives the data and is capable of showing which keys are valid for the vehicle. The display unit could also display other messages, such as, for example "Key validation completed," and may include controls allowing a user of the vehicle to recall a display showing the valid keys, for example, key A, B, and C.

If the lost or stolen key 4 is recovered, the key can be revalidated or reactivated by bringing all the keys into the vehicle again and placing ECU 2 in the key validation mode in order to execute the above-explained key validation procedure. The enable flag for the found key 4 will then be set in EEPROM 12.

To avoid the requirement for any additional hardware components to be added to the vehicle, the predetermined procedure used to place ECU 2 in the key validation mode needs to be executed using existing vehicle components. The predetermined procedure should advantageously involve using components and operations which are normally involved in a start or entry procedure for the vehicle. Most vehicles have a

start procedure which involves pressing a pedal 8, which may be the brake or clutch pedal, and then simultaneously turning on an ignition start switch 10 of the vehicle. ECU 2 is connected to the electric network or wiring harness of the vehicle so as to receive signals generated when pedal 8 is depressed and ignition start switch 10 is turned on. The predetermined procedure to enter the key validation mode can then involve the holder of the keys simply depressing pedal 8 and turning on ignition start switch 8 alternately a number of times, say three times, instead of doing this simultaneously. ECU 2 on detecting depression of pedal 8 and turning on of ignition start switch 10 alternately can then generate a message for message unit 6 to confirm entry into the key validation mode when the predetermined procedure has been executed. ECU 2 can also issue cues on message unit 6 to follow the time sequence for depression of pedal 8 and turning on ignition start switch 8, to assist the holder of the keys in correctly executing the procedure to enter the key validation mode. Alternatively the steps and vehicle components used for entry into the vehicle can be used - for example, in some passive security systems the key is excited on lifting a door handle 16. The predetermined procedure required to enter the key validation mode may require a holder of the keys to lift door handle 16 a number of times within a certain period of time, for example four times in two seconds.

ECU 2 can be provided by or divided into a number of ECUs, and similarly the vehicle can include a number of transceivers and antennas to communicate with remote keys 4. Keys 4 may be passive entry keys which require energy from the vehicle in order to communicate with ECU 2 or the keys may have their own battery power supply. Also, whilst the present invention is

particularly advantageous for keys which have no activating buttons, keys 4 can include activating buttons and the security system may be a combination of active and passive security systems. For example, the security system may be designed such that key 4 is able to communicate over a distance, of for example 30 m, with the vehicle when activated, and is also able to be energized or excited when closer to the vehicle by, for example, lifting the door handle, or some other activation device, when in the vicinity of the vehicle.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.